IPsec and VPN

Segurança Avançada de Redes

Mestrado Integrado
Engenharia de Computadores e Telemática
DETI-UA

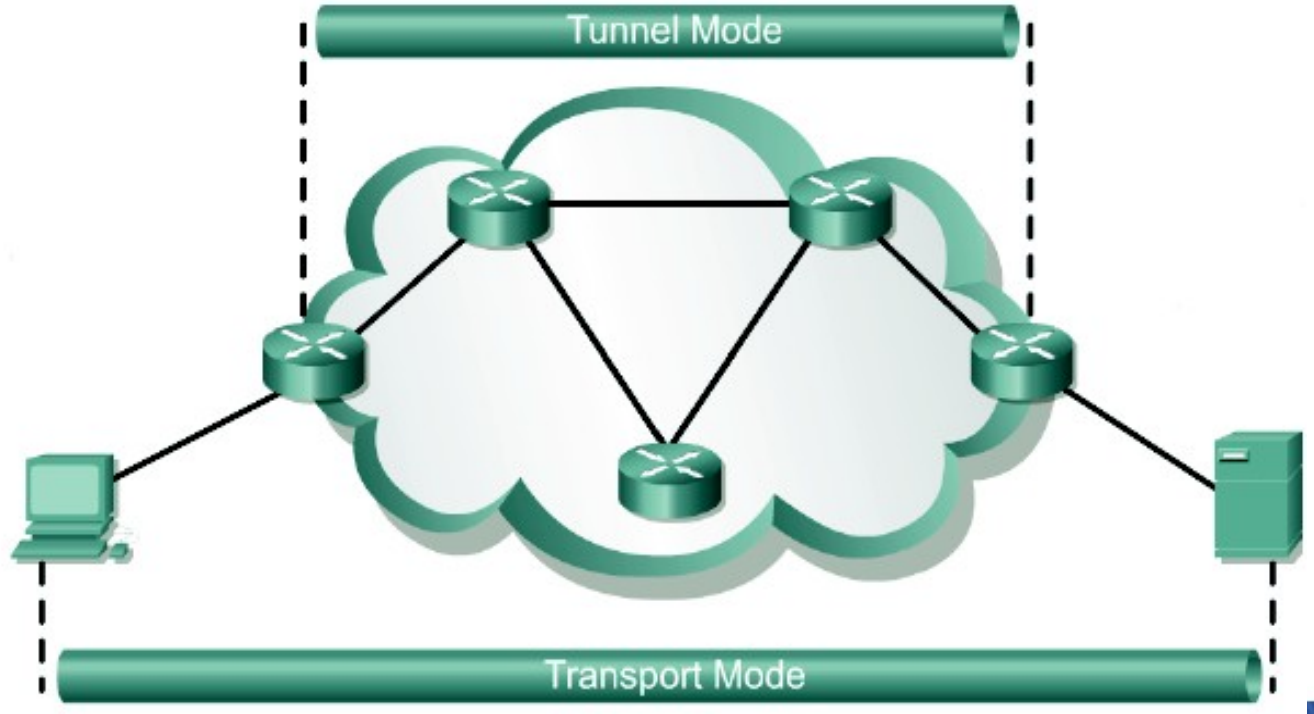
universidade de aveiro
deti.ua.pt

IPSec

- Framework of security protocols and algorithms used to secure data at the network layer
- Authentication Header (AH)
  - Ensures data integrity
  - Does not provide confidentiality
  - Provides origin authentication
  - Uses Keyed-hash mechanisms
- Encapsulating Security Payload (ESP)
  - Provides data confidentiality (encryption)
  - Data Integrity
  - Does not protect IP header
- AH and ESP use symmetric secret key algorithms, although public key algorithms are feasible

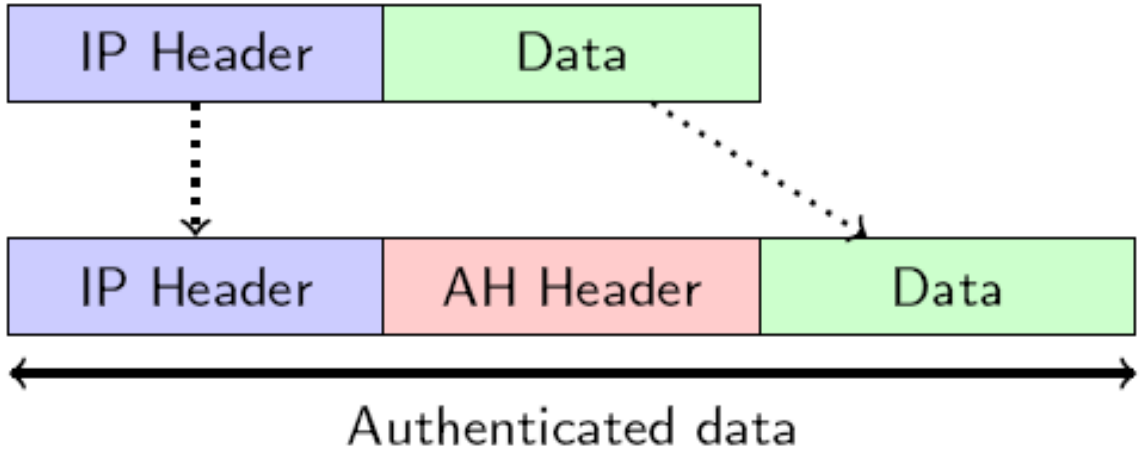
IPSec Modes

- Tunnel
  - IPSec gateways provide IPSec services to other hosts in peer-to-peer tunnels
  - End-hosts are not aware of IPSec being used to protect their traffic
  - IPSec gateways provide transparent protection over untrusted networks
- Transport
  - Each end host does IPSec encapsulation of its own data, host-to-host.
  - IPSec has to be implemented on end-hosts
  - The application endpoint must also be the IPSec endpoint

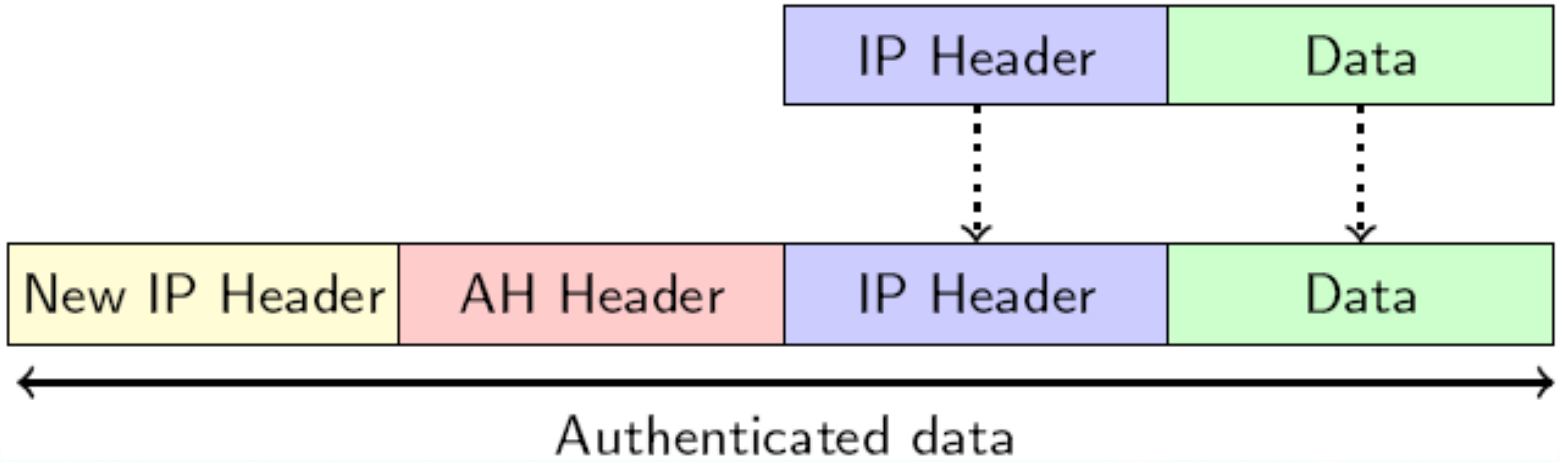


IPSec - AH header placement

- Transport mode

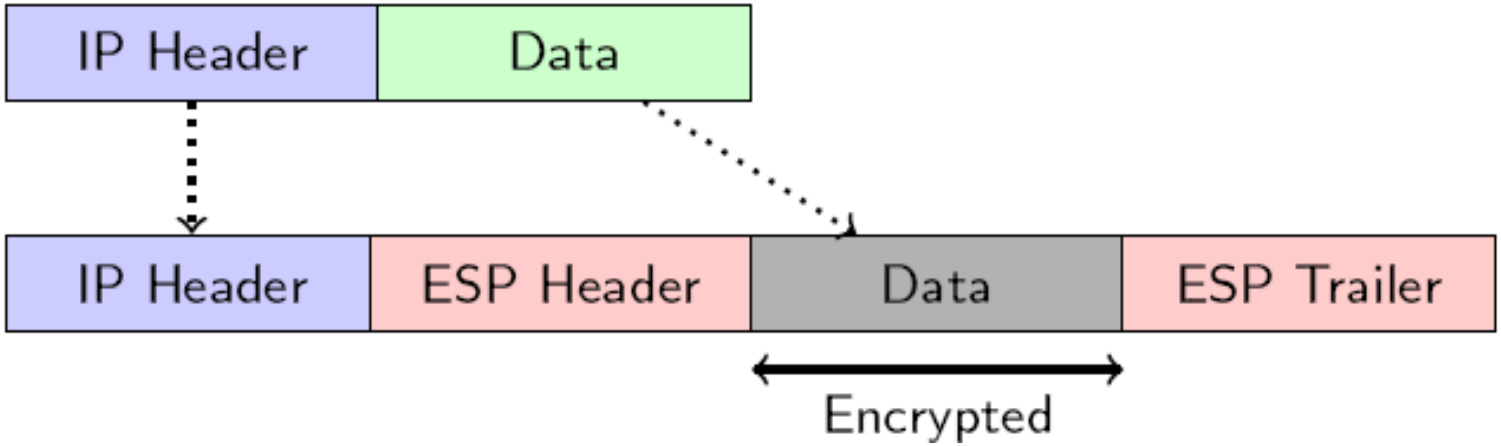


- Tunnel mode

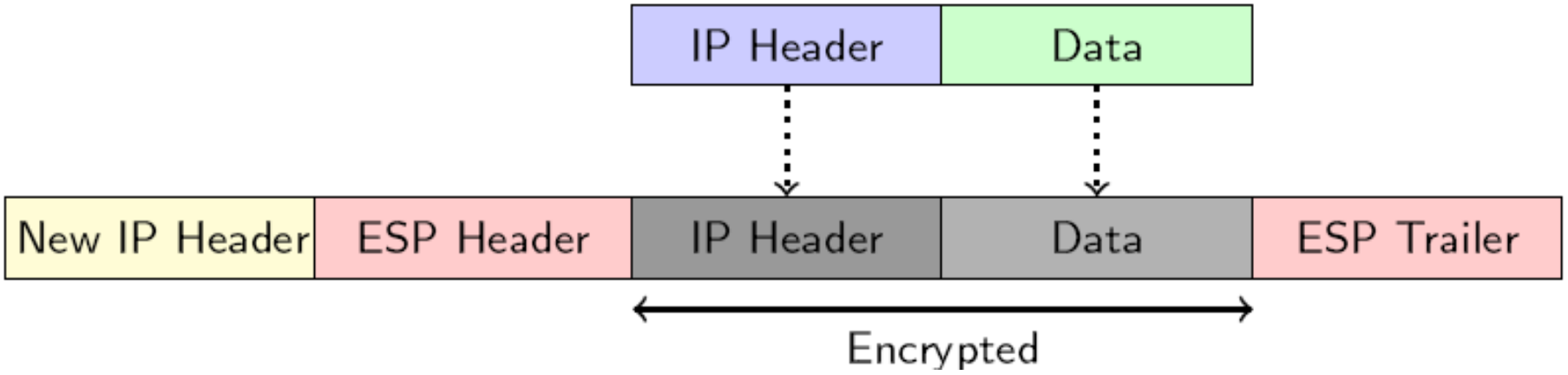


IPSec - ESP header placement

- Transport mode



- Tunnel mode



IPSec - Security Associations

- SAs represent a policy contract between two peers or hosts
- Describe how the peers will use IPSec security services to protect network traffic
- An SA contains the following security parameters:
  - Authentication/encryption algorithm, key length and other encryption parameters (e.g. key lifetime, ...)
  - Session keys for authentication, or HMACs, and encryption, which can be entered manually or negotiated automatically
  - A specification of network traffic to which the SA will be applied (e.g. IP traffic or only TELNET sessions)
  - IPSec AH or ESP encapsulation protocol and tunnel or transport mode

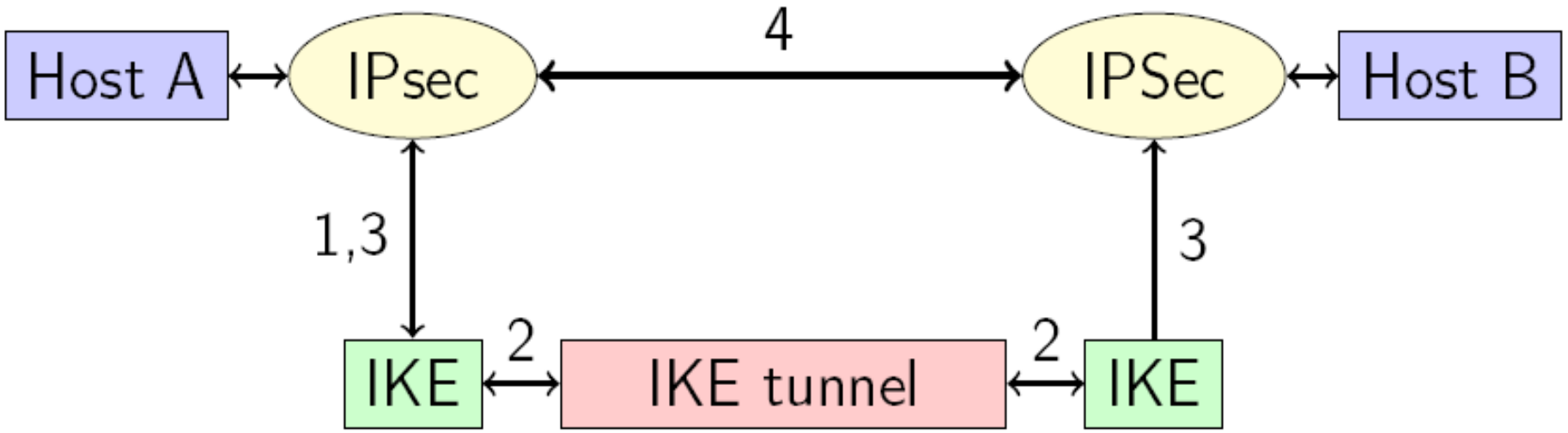
Establishing SA and Cryptographic Keys

- ISAKMP - Internet Security Association and Key Management Protocol
  - Used to establishing Security Associations (SA) and cryptographic keys
  - Separate the details of security association management (and key management) from the details of key exchange
  - Provides a framework for authentication and key exchange but does not define them
- Oakley Key Determination Protocol
  - Key-agreement protocol
  - Allows authenticated peers to exchange keying material across an insecure connection
  - Uses Diffie-Hellman
- SKEME
  - Key exchange protocol
- IKE - Internet Key Exchange
  - Is a hybrid protocol
  - Uses part of Oakley and part of SKEME in conjunction with ISAKMP

IKE and IPsec

- Enhances IPSec by providing additional features and flexibility
- Provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations
- The IKE tunnel protects the SA negotiations. After the SAs are in place, IPSec protects data transference
- Advantages
  - Eliminates the need to manually specify IPSec security parameters at both peers
  - Allows administrators to specify a lifetime for the IPSec security association
  - Allows encryption keys to change during IPSec sessions
  - Allows IPSec to provide anti-replay services
  - Permits certification authority (CA) support for a manageable, scalable IPSec implementation
  - Allows dynamic authentication of peers
- IKE provides three methods for two-way authentication:
  - Authentication using a pre-shared secret (PSK)
  - Authentication using RSA encrypted nonces
  - Authentication using RSA signatures

IKE and IPsec



IKE and IPsec – Modes

- IKE modes control an efficiency versus security tradeoff during initial IKE key exchange
- Main mode
  - Requires six packets back and forth
  - Provides complete security during the establishment of an IPsec connection
- Aggressive mode
  - Uses half the exchanges
  - Provides less security because some information is transmitted in cleartext

IKE and IPsec

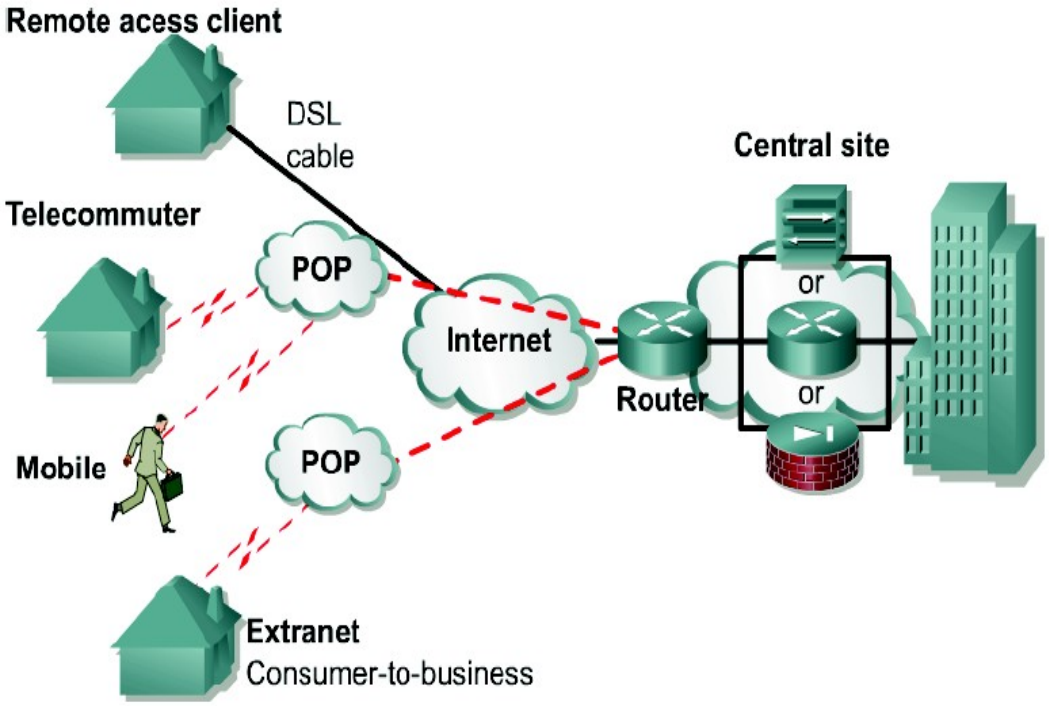
- Enhances IPSec by providing additional features and flexibility
- Provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations
- The IKE tunnel protects the SA negotiations. After the SAs are in place, IPSec protects data transference
- Advantages
  - Eliminates the need to manually specify IPSec security parameters at both peers
  - Allows administrators to specify a lifetime for the IPSec security association
  - Allows encryption keys to change during IPSec sessions
  - Allows IPSec to provide anti-replay services
  - Permits certification authority (CA) support for a manageable, scalable IPSec implementation
  - Allows dynamic authentication of peers
- IKE provides three methods for two-way authentication:
  - Authentication using a pre-shared secret (PSK)
  - Authentication using RSA encrypted nonces
  - Authentication using RSA signatures

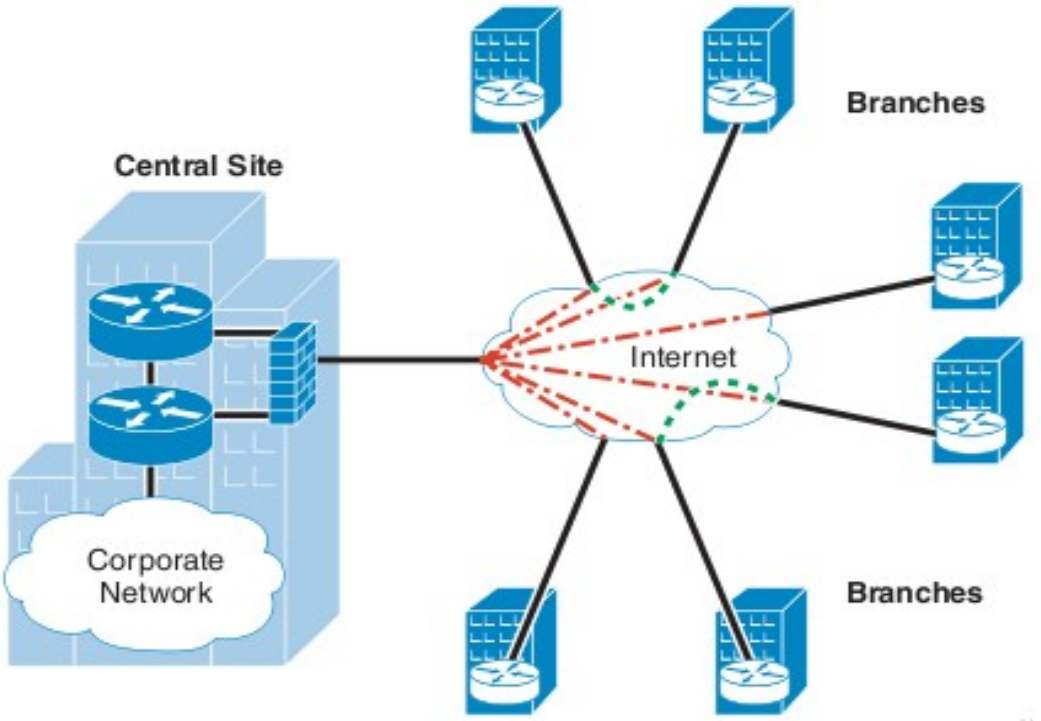
Network Service and Systems

Virtual Private Networks

VPN - Virtual Private Networks

- Is an encrypted connection between private networks over a public network





- Remote Access VPN
- Site-to-Site VPN

VPN types

- Remote Access VPN
  - PPTP
  - L2TP/IPsec
  - SSL/TLS VPN
    - Web VPN (client-less SSL VPN) – VPN client can be a standard browser
  - SSH VPN
  - Open VPN
- Site-to-Site VPN
  - IPsec VPN
    - With static or dynamic configuration
  - IPsec + GRE VPN
    - Dynamic Multipoint VPN

Remote Access VPN - PPTP VPN

- Based on PPTP
  - PPTP packages data within PPP packets
  - Encapsulates the PPP packets within IP packets
- Uses a form of General Routing Encapsulation (GRE) to get data to and from its final destination
- Supports authentication based on protocols PAP, EAP, CHAP, MS-CHAPv1 and MS-CHAPv2
- Uses MPPE as cipher
  - Has two different keys (one for each direction)
  - Requires MS-CHAPv2 authentication
  - Keys derived from the MS-CHAPv2's password hash and challenges
- PPTP creates a TCP control connection between the VPN client and VPN server to establish a tunnel
  - Uses TCP port 1723 for these connections
- PPTP can support only one tunnel at a time for each user

Remote Access VPN - L2TP/IPSec VPN

- Authentication can be performed with Digital Certificates (RSA) or with the same PPP authentication mechanisms as PPTP
- Provides data integrity, authentication of origin and replay protection
- Encryption provided by IPSec (ESP protocol)
- Can support multiple, simultaneous tunnels for each user
- Slower performance than PPTP

Other Remote Access VPN types

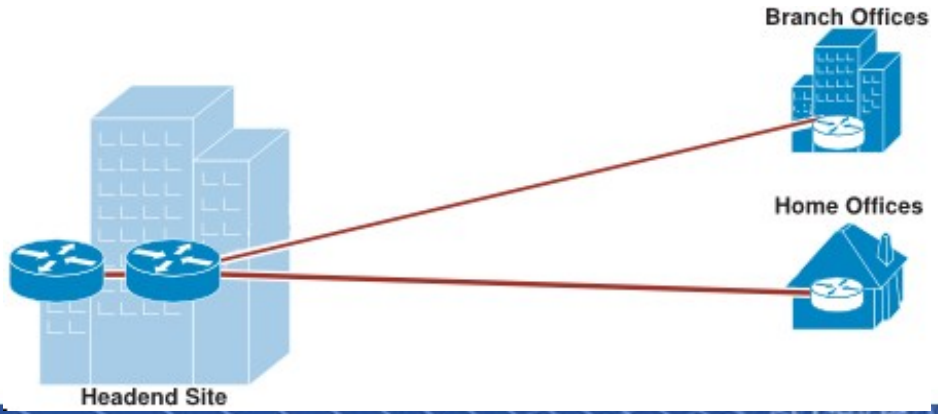
- SSL/TLS VPN
  - SSL/TLS protocol handles the VPN tunnel creation
  - SSL/TLS is much easier to implement than IPSec and provides a simple and well-tested platform
  - RSA handshake (or DH) is used exactly as IKE in IPSec
- SSH VPN
  - VPN over a SSH connection
  - SSH tunneling - port forwarding
- OpenVPN
  - Implements a SSL/TLS VPN
  - Allows PSK, certicate, and login/password based authentication
  - Encryption provided by OpenSSL (can use all ciphers available)
  - Compatible with dynamic and NAT addresses

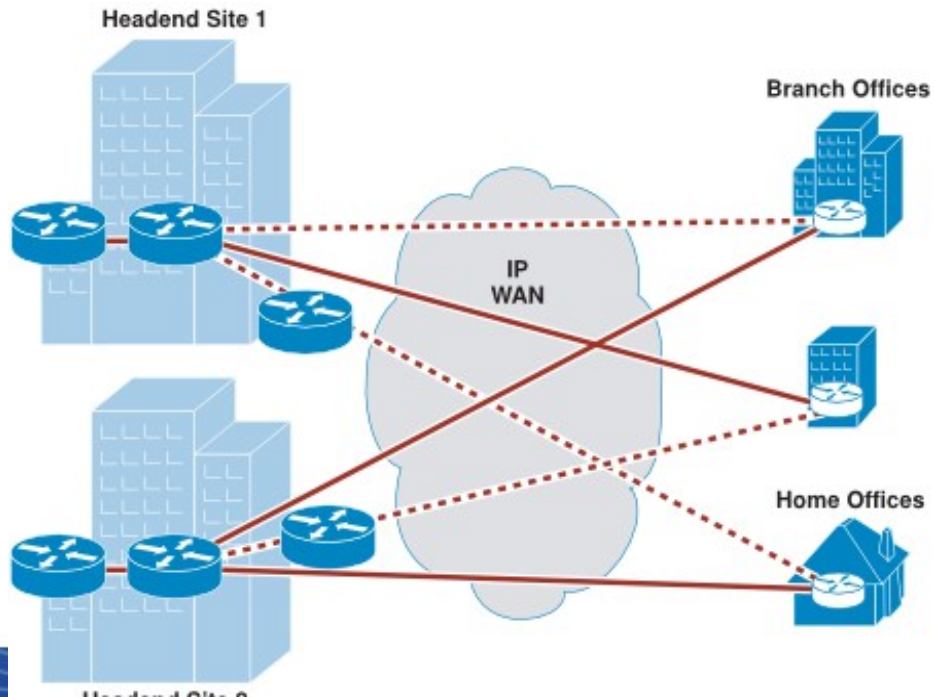
Variants of Site-to-Site IPsec VPN

- IPsec tunnels with static configuration
  - Requires the knowledge of all peers (IP addresses and security parameters)
  - High configuration overhead
- IPsec tunnels with dynamic configuration (at the headend/hub)
  - Hub + spokes configuration
  - Generic configuration at the headend/hub
  - Easy to add new spokes

→ A basic IPsec tunnel can't protect multicast traffic.

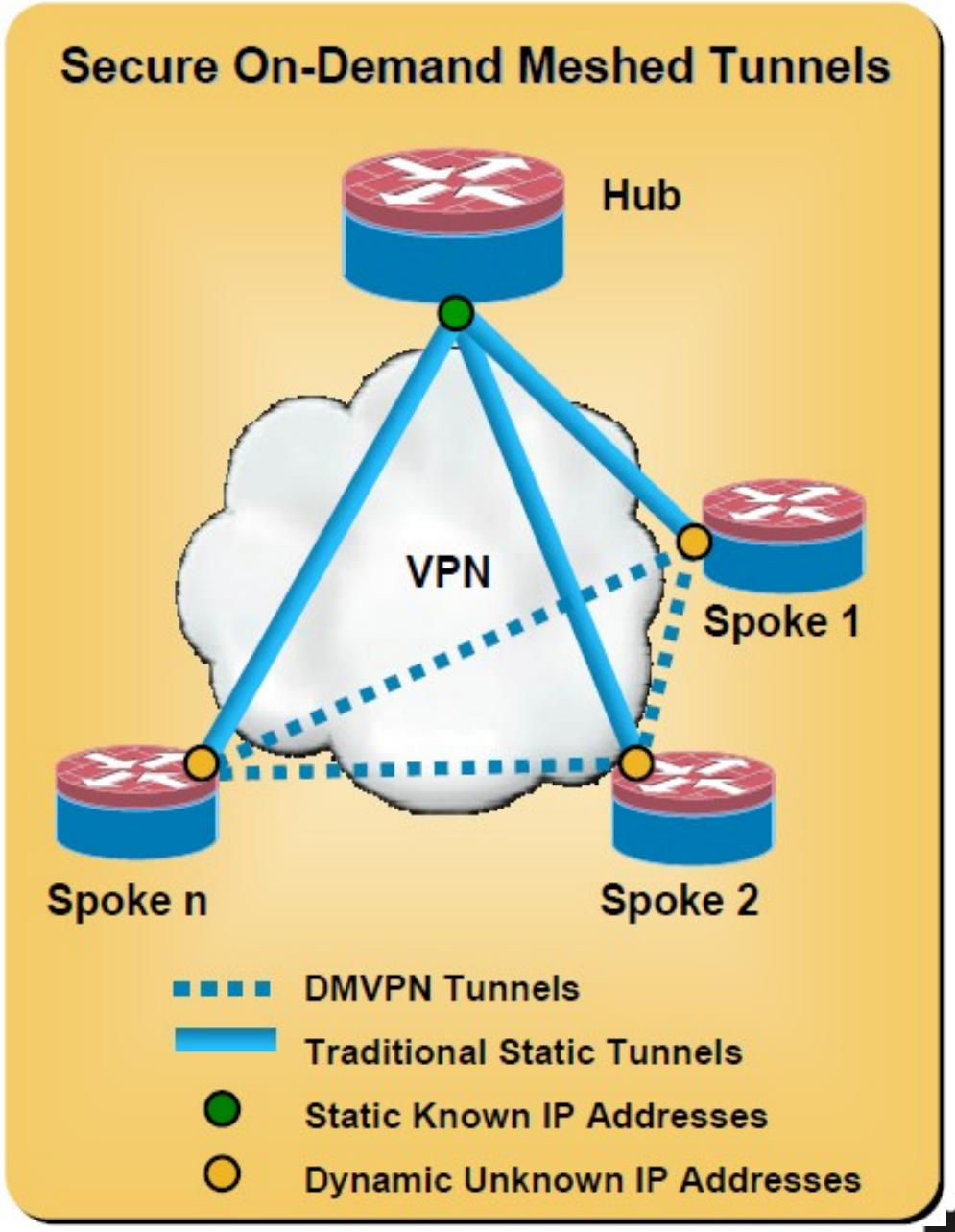
- IPsec + GRE tunnels
  - Generic Routing Encapsulation (GRE) allows the protection of multicast traffic over IPsec
  - Dynamic Multipoint VPN (DMVPN)





Dynamic Multipoint VPN

- Provides full meshed connectivity with simple configuration of hub and spoke
- Supports dynamically addressed spokes
- Facilitates zero-touch configuration for addition of new spokes
- Features automatic IPsec triggering for building an IPsec tunnel



DMVPN

- DMVPN relies on two proven technologies:
  - Next Hop Resolution Protocol (NHRP)
    - Creates a distributed (NHRP) mapping database of all the spoke tunnels to real (public interface) addresses
  - Multipoint GRE (mGRE) Tunnel Interface
    - Single GRE interface to support multiple GRE and IPsec tunnels
    - Simplifies size and complexity of configuration
- Dynamic Tunnel Destination simplifies support for dynamically addressed spokes
  - NHRP registration and dynamic routing protocols
- No need to touch the hub for new spokes
- Spoke to spoke traffic via the hub or direct

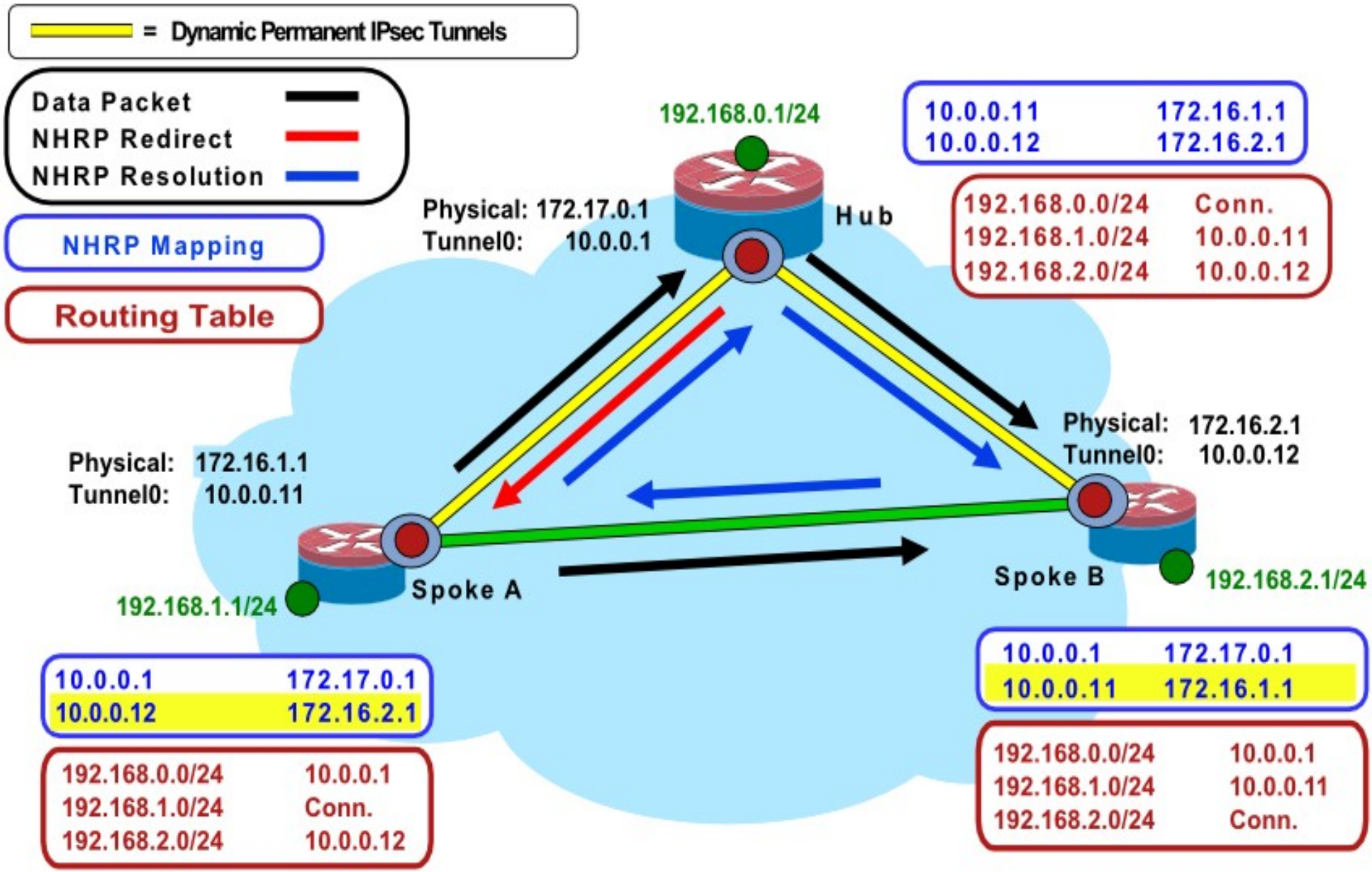
Next Hop Resolution Protocol (NHRP)

- Creates a distributed (NHRP) mapping database of all the spoke tunnels to real (public interface) addresses
- NHRP registration
  - Spoke dynamically registers its mapping with NHRP server
  - Supports spokes with dynamic addresses or NAT
- NHRP resolutions and redirects
  - Supports building dynamic spoke-to-spoke tunnels
  - Control and IP Multicast traffic still through hub
  - Unicast data traffic direct
    - Reduced load on hub routers

Dynamic Addressing

- Spokes have a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes
  - They register as clients of the NHRP server
- When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it queries the NHRP server for the real (outside) address of the destination spoke
- The originating spoke can initiate a dynamic GRE/IPsec tunnel to the target spoke (because it knows the peer address)
- The spoke-to-spoke tunnel is built over the mGRE interface

NHRP - example



DMVPN network designs